Magistrate Judge Brian A. Tsuchida

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

CHRISTOPHER A. SCHROEBEL ,

Defendant.

CASE NO. MJ11-566

COMPLAINT

Title 18, U.S.C.

Sections: 1030(a)(2),1030(c)(2)(B)(ii), 1029(a)(2),1029(c)(1)(A)(i), and 1028A(a)(1)

FILED UNDER SEAL

BEFORE BRIAN A. TSUCHIDA, United States Magistrate Judge, U. S. Courthouse, Seattle, Washington.

The undersigned complainant being duly sworn states:

COUNT ONE
(Obtaining Information From a Protected Computer)

Beginning on a date uncertain, but on or about July 20, 2011, and continuing until on or about August 3, 2011, within the Western District of Washington and elsewhere, CHRISTOPHER A. SCHROEBEL intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, to wit, he intentionally accessed a credit card processing computer belonging to and located at Mondello's Italian Restaurant, in Seattle, WA, and obtained therefrom credit card track data that included credit card numbers belonging to K.H., K.W., J.H., V.D., S.J., and

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

M.H., and that he committed such offense in furtherance of a criminal and tortious act in violation of the Constitution and laws of the United States, specifically, access device fraud, in violation of Title 18, United States Code, Section 1029(a)(2).

All in violation of Title 18, United States Code, Section 1030(a)(2) and 1030(c)(2)(B)(ii).

COUNT TWO
(Access Device Fraud)

Beginning on a date uncertain, but on or about July 20, 2011, and continuing until on or about August 8, 2011, within the Western District of Washington and elsewhere, CHRISTOPHER A. SCHROEBEL, knowingly and with the intent to defraud, trafficked in and used credit card track data from credit card accounts belonging to K.H., K.W., J.H., V.D., S.J., and M.H., without their knowledge or consent, and by such conduct, from on or about July 20, 2011 to August 8, 2011, obtained profits aggregating $1,000.00 or more, said trafficking affecting interstate and foreign commerce, in that the credit card account numbers that were so trafficked and used were used by CHRISTOPHER A. SCHROEBEL and others to make fraudulent purchases in states outside the State of Washington.

All in violation of Title 18, United States Code, Section 1029(a)(2) and 1029(c)(1)(A)(i).

COUNT THREE
(Aggravated Identity Theft)

On or about July 28, 2011, within the Western District of Washington and elsewhere, CHRISTOPHER A. SCHROEBEL knowingly transferred, possessed and used, without lawful authority, a means of identification of another person, to wit, the personally identifiable credit card number of ****-****-****-9563, belonging to M.H., of Seattle, WA, during and in relation to a felony listed in Title 18, United States Code,

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Section 1028A(c), to wit, Access Device Fraud, in violation of Title 18, United States Code, Section 1029.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

And the complainant states that this Complaint is based on the following information:

I, DAVID DUNN, being first duly sworn on oath, depose and say:

A. Case Summary

1. The Seattle Police Department has been actively investigating unauthorized computer intrusions ("hacks") into the computer systems of small businesses located in the Western District of Washington. The known victim businesses, to date, include Mondello's Italian Restaurant, in the Magnolia neighborhood of Seattle, and also the Seattle Restaurant Store, in Shoreline, Washington.

2. The person/s responsible for the hacks installed malicious software ("malware"[1]) on the computer systems of the victim businesses. The malware was designed to, and has collected credit card account numbers belonging to customers/clients of the victim businesses. The stolen credit card account numbers were then transmitted over the Internet to a computer server under the control of the hacker/s and/or their associates. The hacker/s and/or their associates then harvested the stolen credit card account numbers from the server computer to which they had been transmitted. The credit card numbers stolen through these means were then used fraudulently at various locations throughout the United States, causing financial losses to the banks that issued the credit card numbers, including the Boeing Employees Credit Union, a financial

[1]"Malware" is malicious computer code running on a computer. Relative to the owner/authorized user of that computer, malware is computer code that is running on their system that is unauthorized and present on the system without their consent. Malware can be designed to do a variety of different things, including logging every keystroke on a computer, stealing financial information or "user credentials" (passwords or usernames), or commanding that computer to become part of a network of "robot" or "bot" computers known as a "botnet." In addition, malware can be used to transmit data from the infected computer to another destination on the Internet, as identified by an IP address. Often times, these destination IP addresses are computers that are controlled by cyber criminals.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

institution in the Western District of Washington.

B. Agent Background and Sources of Information

3. I am a Police Detective with the Seattle Police Department, and have been such since October of 2000. Before promotion to Detective, I served for 4 years as a Patrol Officer with the Seattle Police Department. In April of 2005, I was transferred to the Seattle Police Department Fraud unit as a Computer Forensic Detective. I am currently, and since October of 2006 have been assigned as a full time member of the USSS Electronic Crimes Task Force, Seattle Field Office. I hold a Special Deputation appointment through the United States Marshals Service that permits me to seek and execute arrest and search warrants supporting a federal task force. As a member of the Seattle USSS E-Crimes Task Force, I investigate violations of federal law in the state of Washington that fall under the responsibility of the USSS, with an emphasis on crimes involving computers, the Internet, and electronic communications.

4. In 1999, I received a BA degree in Social Science from Washington State University. I received my basic law enforcement training through the Washington State Law Enforcement Academy. Since then, I have received additional training in general criminal investigations and fraud and forgery, and hundreds of additional hours of specialized training in the areas of computer forensics, computer hardware, computer software, networking, network intrusion and electronic crimes. I have attended both A+ Software and A+ hardware training, as well as Computer Forensics Core competencies through the Cyber Security Institute. I am certified as an ECSLP (Electronic Crimes State and Local Program) investigator through the USSS and have attended the Department of Defense's INCH and IRC courses as well as the Intermediate Encase (forensic examination software) course.

5. My training and experience also specifically includes training and experience regarding computer and network intrusions, commonly known as "hacking." This includes completion of the 40 hour "Incident Handling and Response" course on network intrusions and incident response through the Department of Homeland Security.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

I have experience with packet analysis, malware and viruses. I am a Certified Ethical Hacker. I have attended 104 hours of training in Network Intrusion Response at the National Computer Forensic Institute. I hold the following forensic certifications: EnCE (EnCase Certified Examiner), ACE (Access Data Certified Examiner) CFCE (IACIS Computer Forensic Certified Examiner). I have received advanced training in both network intrusion forensics as well as Point of Sale forensic investigations.

6. As a member of the USSS E- Crimes Task Force, I have worked on numerous computer and network intrusion cases. These cases have involved a range of hacker techniques and modus operandi, including social engineering, SQL injection attacks, botnet attacks, malware infections and various other means of computer infection and attack. I have examined myriad server logs and volumes of Internet Protocol ("IP") address information as part of my investigation of various hacking cases. I have also created and examined forensic images of dozens of infected and hacked computers and servers. I have investigated cyber cases involving both national and international victims and suspects. As a result, I am familiar with schemes involving large scale Internet crimes and network attacks.

7. I am an investigative or law enforcement officer of the United States within the meaning of Section 3056 of Title 18, United States Code, in that I am empowered by law to conduct investigations, apply for search warrants, and to make arrests for federal felony offenses.

8. The information contained in this affidavit is based upon my personal knowledge and observations, my training and experience, information provided to me by other Seattle police detectives and officers and employees, other federal agents, and a review of documents and records. Because this affidavit is made for the limited purpose of obtaining a complaint, I have not set forth every fact I know concerning this investigation. Rather, I have stated only those facts I believe necessary to establish probable cause that CHRISTOPHER SCHROEBEL has committed violations of Title 18, United States Code, Sections 1030(a)(2), 1030(c)(2)(B)(ii); 1029(a)(2); 1029(c)(1)(A)(i)

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

and 1028A(a)(1).

C. Technical Background

Web Servers and Web Server Hosting Companies

9. Based on my training and experience, I know the following:

10. Websites are hosted on server computers known as **"web servers."** The web server contains the information needed to create the webpage, including the images, text and formatting data. It can also host or hold files available for download. Consumers typically interact with a web server over the Internet, using an Internet browser program such as Internet Explorer.

11. Many individuals and companies want to have websites, but do not want to maintain their own computer server hardware or deal with the security, power, connectivity and other issues associated with keeping a website online 24/7. They will instead lease a web server from a **web server hosting company**, also known as "web hosting" companies.

12. **Web hosting companies** are companies that own (or lease) computer servers that they in turn lease (or sublease) to customers. The web hosting company typically maintains one or more colocation facilities which house their servers. These locations have all of the necessary power, backup power, security and Internet connections to maintain customer servers and service, 24/7. A web hosting company's customers can be anywhere in the world, because they can administer their leased server/s "remotely," over the Internet.

13. **File Transfer Protocol ("FTP").** FTP is a method of transferring files across the Internet. FTP is used to send larger-sized files, and users typically use a special program to transfer files using FTP. Most Internet users do not knowingly use FTP; rather, it is typically used instead by system administrators and other advanced computer users.

//

Point of Sale Systems

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

14. Point of sale **("POS")** computer systems are computer networks that are used primarily by retail businesses and restaurants for processing customer transactions. POS systems integrate the purchase of, and payment for goods or services, to include processing credit card transactions.

15. A typical POS system has two distinct parts, a POS terminal and a POS "back of house server." The POS terminal is the computer that is used by employees to input customer orders, and to swipe credit cards or input a cash payment amount. The POS terminal then transmits that data to the back of house server. Once it reaches the back of house server, the data is encrypted and transmitted, over the Internet, to the businesses merchant card processor, which then verifies the card and also processes the transaction with the relevant banks.

16. POS systems are typically connected directly and constantly to the Internet, in order for the businesses to obtain immediate authorizations for transaction from their merchant card processor before the customer signs the receipt and leaves the premises. In most cases, both the POS terminal and back of house server are a program running on a Microsoft operating system.

17. I have been investigating POS network intrusions for several years and, as a result, have learned that there is similar Modus Operandi associated with most of them.

18. The first commonality is the manner and means for gaining unauthorized access to ("hacking") the POS system. Most POS systems include some kind of remote access capability. This is a convenience to both the business with the system and the POS system vendor, because POS systems can sometimes break and in order for a business to get its system back up and running quickly, the manufacturer or service technician will often connect to the system from a remote location in order to fix the computer. This saves both time and money as companies can have an almost immediate response and don't have to wait for someone to physically come to their business location.

//

19. I have learned, however, that this remote access capability can also be a

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

vulnerability for the merchant, because if the system is not properly secured, hackers can use this same remote access capability to hack into the computer system and take full control of the system and install malware on it.

20. Once malware has been installed, the hacker is able to collect and steal customer credit card data, and then to resell the stolen credit card numbers for fraudulent use by others, or to use it him/herself for fraud, or to pass it on to criminal associates or coconspirators for fraudulent transactions.

21. I have also learned through my experience with these cases that hacks of POS systems often go undetected by the victim businesses for months, until either multiple customers have complained that their credit card number was stolen during use at the business, or until a financial institution notices an increase in fraud associated with a particular business, and reports that to law enforcement.

1&1 Internet, Inc.

22. In my training and experience, I have learned that 1&1 Internet provides a variety of computer hosting services to the general public, including web hosting services.

23. In general, any person can contact 1&1 Internet and, for a fee, lease a server located at a 1&1 Internet facility. 1&1 Internet will then provide that customer with logon credentials for that server and will allow the customer to administer the server; that is, to configure, and to upload and download data to the server, as the customer sees fit.

24. Because 1&1 Internet owns the server and the facility where the server is located, any Internet traffic between the world wide web and their customers' servers will appear to be traffic to 1&1 Internet, rather than the actual end customer.

D. Details of Probable Cause

Hack of POS System of Mondello's Restaurant in Seattle, WA

25. On August 6, 2011, C.B., the owner of Mondello's Italian Restaurant in Seattle, Washington called the Seattle Police Department ("SPD") to report a possible computer intrusion at his restaurant. C.B. told SPD Officer Dornay that he had received numerous complaints from customers about fraud on their credit cards and that he, C.B.,

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

believed that his restaurant computer system had been hacked and that customer credit card account numbers had been stolen. C.B. provided Officer Dornay with a list of six customers who had reported fraud on their credit cards. All six customers reside in the City of Seattle.

26. Officer Dornay contacted several of the victims by phone and learned the following.

a) K.H. went to Mondello's on July 31, 2011 and used her credit card to purchase food. On that same day, her credit card was used at several different locations in California including Home Depot, Wal-Mart, Jack-n-the-Box, and several other locations. The total fraud on her card was over $600.

b) K.W. ate at Mondello's during the same time period. Her card was also used for fraudulent transactions in California.

c) J.H. dined at Mondello's during the same time period. His credit card was used in several fraudulent transactions in southern California.

d) Victims V.D. and S.J. dined together at Mondello's on July 30, 2011 and both had their individual cards used for fraud at locations in southern California on July 31, 2011.

27. I spoke with an investigator at the Boeing Employees Credit Union ("BECU"). He told me that between July 20, 2011 and August 8, 2011, seven credit cards issued by BECU used at Mondello's restaurant had subsequent fraud loss. I reviewed the fraud loss data and found that there was $562 in actual loss on the cards and an additional $1974.50 in attempted transactions. I followed up with phone calls to two of the victims. I contacted card holder K.H. by phone and learned that his BECU Mastercard ending in **8760 had been used without his authorization, in California. K.H. had eaten at Mondello's on August 3, 2011, and the fraud occurred on August 5, 2011. I contacted cardholder M.H. by phone and learned that her BECU Mastercard ending in **9563 had been used without her authorization, in California. M.H. had eaten at Mondello's on July 28, 2011, and the fraud occurred on July 29, 2011.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

28. I also spoke with an investigator for American Express who told me that they had fraud related to cards used at the restaurant from March of 2011 through September of 2011. That fraud was in excess of $10,000.00.

29. On September 22, 2011, I contacted C.B. regarding the possible hack of his POS system. C.B. reported that in August, he had contacted a local computer company to come in and take a look at his computer system. C.B. stated that E.G. of Magnolia Tech Outlet responded and examined the computer hard drive. C.B. said that E.G. did locate some kind of malicious software. I asked for and received C.B.'s permission to contact E.G. and ask him additional questions about the incident.

30. On September 22, 2011, I spoke with E.G. on the phone. E.G. reported that he had examined the computer hard drive from the POS system at Mondello's Restaurant. He reported that he did locate evidence of keystroke logging software on the computer system. E.G. reported further that he did not reinstall that hard drive in the computer, but rather that he had put a new, uninfected hard drive in the computer and retained the original hard drive, which he still had in his possession.

31. I recontacted C.B., and asked if he would consent to a search of that hard drive for evidence related to the credit card fraud. C.B. said that he would allow the search.

32. On September 22, 2011, I contacted C.B. at his restaurant, at which time he showed me the computer that had been hacked. C.B. also told me about his computer network and credit card processing system. C.B. said that the intrusion had been a stressful event for him. He was concerned about his business reputation and the loss of customers due to the event. C.B. signed a consent to search form for the computer hard drive.

33. I left the restaurant and walked over to Magnolia Tech Outlet, where E.G. released custody of the hard drive from Mondello's, to me. E.G. told me that he had run scans on the hard drive and had found keystroke logging software on the computer.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

34. On September 22 and 23, 2011, I conducted a preliminary forensic examination on the computer hard drive from Mondello's, and noted several items of interest on the computer.

35. First, I noted that there were at least two possible means to gain remote access to the computer system. One was through Microsoft Remote Desktop software. This software comes standard on most Microsoft operating systems. For security purposes, however, it is turned off, by default. I noted that on this computer, it was turned on. This meant that the credit card processing computer could be accessed from the Internet if the attacker had the correct password. I also saw that there was a second remote software installed on the computer called, "log me in." "Log me in" is a commercially available, third party remote access software that allows people to access a computer remotely.

36. Based on reports of fraud beginning on July 31, 2011, I began to work backwards and look for software that could have been used to steal credit card information. I reviewed the log files from the scans that E.G. had conducted and saw that his scans had found and deleted a program called, "Ardamax." Ardamax is a commercially available keystroke logging software.

37. Based on my training and experience, I know that when a credit card is used at many POS terminals, the credit card reader actually converts the reading of the magnetic card data in keystrokes that are transmitted to the computer. Keystroke logging software is able to read this information and then transmit the data to a third party.

38. In this case, I found that on July 20, 2011, at around 0200 hours, a subject with control of the Mondello computer had directed the web browser of the Mondello's system to the website, "www.scripters.in," and that from this site he/she had downloaded a file called, "a8.exe." This file was no longer present on the Mondello's computer. However, using a government computer, I was able to type in that website address, go to the website, and then download that same piece of computer code.

//

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

39. I investigated the website that was hosting www.scripters.in and the "a8.exe" malware. I found that the site was registered to a company in Washington DC, named, "Web Services PVT LTD." I attempted to telephone the number listed and received a message stating that the "magic jack"[2] customer was "not available." I know that computer hackers and other online criminals will often use third party companies to register their domain names in order to protect their identities.

40. I conducted a traceroute command against the server to determine the IP address of the server hosting the website, www.scripters.in. I found that the site was being hosted at IP address, 74.208.193.165. I then learned that this IP address belongs to 1&1 Internet, a computer server hosting company, located in Chesterbrook, Pennsylvania.

41. After downloading the malware and moving it to an exam machine, my antivirus software immediately flagged it as "Ardamax" keystroke logging software and tried to delete it from my computer. I installed it on a virtual computer with no antivirus software and found that after double clicking on the a8.exe, the program installed a second program on my computer called, "LGDI.exe." I reviewed connections that my computer was making to the Internet and found that LGDI.exe was communicating to IP address 74.208.193.165 using a specific kind of communications protocol called "FTP." I immediately noted that the server it was connecting to was the same IP address from which I had downloaded the software.

42. The fact that the malware had been downloaded from the same location as that to which it was also sending the stolen information made it clear to me that the server, www.scripters.in, was controlled by the same individual/s who had stolen the credit card numbers from Mondello's.

43. I reviewed publically available information about the Ardamax software and found that it was capable of storing keystrokes and screen captures from a victim

---

[2]I know from my training and experience that "magic jack" is a Voice Over Internet telephone system. A user can purchase a "magic jack" and connect it to their home Internet connection or they can connect it directly to their computer. Using the magic jack a person can make and receive phone calls from anywhere in the world using the same phone number at a very low cost.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

computer and then saving the stolen information as a text or web document. It is also capable of sending the information using either a well known e-mail protocol or via the FTP protocol.

44. My next step was to capture all of the Internet traffic from my infected examination computer. I reviewed this captured data and what I found was a series of communications, as follows:

a) My computer asked my Internet service provider to give it the IP address of the website, www.scripters.in.

b) My Internet service provider responded to my computer that www.scripters.in was located at IP address 74.208.193.165. (1&1 Internet).

c) My computer contacted www.scripters.in at that IP address and told the www.scripters.in server that it wanted to communicate using the FTP protocol, in order to send www.scripters.in data from my computer.

d) My computer then told www.scripters.in that it wanted to connect to the FTP server using a username of "scripter" and a password of "iamcheese."

e) My computer then transferred a file to the www.scripters.in server with information that it had captured from my computer.

45. Based on my training and experience, I know that the username and password of "scripter" and "iamcheese" are not a default combination used by any known computer program, but rather a username and password that were programed into the a8.exe malware. Additionally, in order to actually communicate and receive the file, the www.scripters.in server would have to have been preprogrammed with that username and password.

46. During my investigation, I found that if I typed www.scripters.in into a standard computer web browser, a connection would be made, but that I would just see a blank screen. Based on my training and experience, I believe this signifies that it's not a website intended to be viewed or used by the general public, but is instead a website that is devoted to the malicious activities described above.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

47. I know also, from my training and experience, that in the computer world, a "scripter" is a person who writes computer codes that are interpreted by a second computer program and executed. Scripters are at the very high end of advanced users, not quite writing actual computer code, but capable of manipulating that code for their own purposes. I know, as well, that most malware is written by computer programmers, and then modified by many different scripters and hackers for their own unique malicious purposes and use.

Hack of POS System of The Restaurant Store, in Shoreline, WA

48. On September 23, 2011, I spoke with Seattle Police Detective Chris Hansen regarding the intrusion at Mondello's Italian Restaurant. I told him that the malware was transmitting data to a server at 1&1 Internet. Det. Hansen told me that remembered seeing a similar connection during a response to a network intrusion that had occurred earlier in the year in Shoreline, WA.

49. In January of 2011, BECU fraud investigators notified Det. Hansen and I of a suspected point of compromise at The Seattle Restaurant Store, located at 14910 Aurora Ave N, Shoreline, WA. They told us that a number of cards that had been used at the store were being used for fraudulent transactions at locations outside of the State of Washington.

50. On January 21, 2011, Det. Hansen and Kirkland Police Detective Carroll went to the business and obtained forensic images of the back of house server, the RAM and a POS system at the business.

51. I reviewed The Seattle Restaurant Store forensic images in the wake of the Mondello's incident, and noted that at the time The Seattle Restaurant Store forensic images were created, there were open connections on their system to IP 74.208.193.165. This is the same IP address that had been used to receive the stolen information from Mondello's restaurant. I also found malware on The Seattle Restaurant Store system, and noted that it was named, "IKNX.exe." I noted that while the name was different than that of the malware on the Mondello system (LGKI.exe), it was a similar name in that it was a

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

four letter combination that did not form a word and was all in caps. I found that the malicious software had been downloaded on The Restaurant Store system on January 6, 2011. I copied the malware from the forensic image to my forensic computer, and the antivirus on my forensic computer immediately flagged the file as the Ardamax Keystroke logging software, just as it had for the LGKI.exe malware.

52. I reviewed the RAM image from the infected computer and found several more items of interest. The first was a web address of "www.crypter.in." The ".in" portion means that the site is registered to the country of India, which was the same as the site found in the Mondello's account. Second, I found that the password used to upload the stolen data was "pwd011491." On September 26, 2011, I conducted a trace route and found that www.crypter.in was being hosted at IP 74.208.193.165, the same IP identified in relation to the Mondello's hack.

53. In reviewing the RAM, I found that the IKNX.exe application was actively stealing credit card information and I found full credit card magnetic stripe data was being stored.

54. I checked the website www.crypter.in, in October of 2011, and found that it showed a white page with nothing but the words "fuck you" listed at the top of the page, a strong indication that this page is not intended for any kind of legitimate Internet traffic.

Records Related to Server at IP Address 74.208.193.165

55. On September 26, 2011, 1&1 Internet provided records that revealed the computer server located at IP 74.208.193.165 was leased by:

Mr. Peter Schroebel
Ultimate Products USA
18909 Sheperdstown Pike, Keedysville, MD 21756
(301) 778-3601

56. The 1&1 Internet records further identified the e-mail address associated with the account as "upg.usa@gmail.com"; indicated that the service was initially ordered on November 13, 2009; and showed that the server was a dedicated Linux Server.

//

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

57. The records provided included abuse complaints that had been received by 1&1 Internet concerning this server. A summary of the relevant complaints is listed below (all of these e-mails addressed to Peter Schroebel at the e-mail address upg.usa@gmail.com):

a) On 05/06/2010, an e-mail from 1&1 Internet to Peter Schroebel stating they are receiving reports of hacking attacks originating from his 1&1 root server.

b) On 05/08/2010, an e-mail from 1&1 Internet to Peter Schroebel stating that, since their last notification, his computer has continued to attack other servers on the Internet and that they have not received an answer to their e-mail dated 05/06/2010. They stated "Your 1&1 Root-Server will therefore be disconnected within 24 hours."

c) On 05/08/2010, an e-mail from "Peter" stating that he had checked for a rootkit[3] and found one running a back end sshd[4] hack with no logs.[5] He stated that he would reimage[6] the server in an hour.

58. Based on my training and experience, this was particularly interesting because 1&1 Internet had not asked him if there were any log files (which would have provided investigative leads). Peter Schroebel appeared to be preemptively telling 1&1 Internet that there were no investigative leads that could be explored in relation to the malicious activity related to his leased server.

---

[3]A rootkit is a type of malware that has administrative control over a computer and can be very difficult to detect and remove. Rootkit malware can hide itself from anti-virus and other software because it has such high level access to the computer.

[4]A SSHD is the server portion of software that allows for secure encrypted communications between two computers. If a personal computer on the Internet wants to communicate with a server in a secure manner, one method would be for that personal computer to use a secure shell (SSH). Using the SSH, the computer would connect to the server which was running SSHD. SSHD is the software running on a server allowing it to accept SSH connections. The server would receive the communication request and the personal computer and the server would then be able to communicate securely.

[5] No logs means that there are no records stored by the software showing who or when any communications occurred.

[6] "Reimage" or "reimaging" a server means that the operating system is reinstalled on the computer. Sometimes computers are so infected with malware, that it is faster and easier to start fresh with a new and clean installation of the operating system, rather than to try and find all of the infected files and remove them.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

d) On 07/19/2010, an e-mail from 1&1 Internet to Peter Schroebel stating that there are hacking attacks originating from his server.

e) On 07/21/2010, an e-mail from 1&1 Internet to UPG.USA@gmail.com informing him that since the previous notification his server has continued to attack other servers and they have not received an answer to the e-mail dated 07/19/2010.

f) On 07/23/2010, an e-mail to Peter Schroebel telling him this is his third ticket in two months and that if it happens again they are going to lock his contract and he will have to reinstall his server.

g) On 05/04/2011, an e-mail from 1&1 Internet to UPG.USA@gmail.com informing him that attacks are emanating from his server. It specifically states that a host at 74.208.193.165 has been banned from the datagram network due to repeated brute force attempts at guessing SSH and/or FTP passwords. The e-mail states, in part, "[T]his strongly indicates that this host is compromised, or that your clients are deliberately engaging in illegal conduct. Please investigate this matter accordingly."

h) On 05/06/2011, an e-mail from Peter Schroebel to 1&1 Internet, in which he responds to the incident listed above, by stating, "We can't see anything wrong on our end. Do you have . . . logs? If you do, then please send them to us as we want to know what is going on so that we can prevent this from happening again."

i) On 05/06/2011, an e-mail from 1&1 Internet to UPG.USA@gmail.com thanking him for "Getting back to us" and informing him that he has three days to address the issue and provide them a short report. 1&1 Internet warns that if no action has been taken the server will be taken offline.

59. Based on my review of the abuse complaints provided, it appears that the requested report was never provided, but that 1&1 Internet did not disconnect his service.

Review of Bank Records

60. The records from 1&1 Internet also included a credit card linked to account #474477********14. I determined, from the number, that this was a Visa card number issued by Bank of America.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

61. Records obtained from Bank of America showed that the Visa card was in fact a debit card linked to a bank account owned by Christopher A. Schroebel. The address of record for this Bank of America account was the same address that was provided to 1&1 Internet by the lessee of the server referenced above. The records also showed the birth date for Christopher Schroebel as January 14, 1991. Another way to view his birthdate is "01-14-91." As noted in paragraph 52 above, the malware installed at The Seattle Restaurant Store had a password of "pwd011491" embedded in its code.

62. Further review of the bank statements associated with the account showed that the account was opened in February of 2011.

63. In February of 2011 there was relatively little activity in the account, and less that $2000.00 in total deposits.

64. In March of 2011 there was a dramatic and significant increase in activity related to the bank account. The total deposits were $33,654.54, and there were debits of $15,427.90. The deposit activity to the account included 22 "counter credit" deposits. Fourteen of the deposits were in increments of $100. The credits ranged from $100 to $1600. There were five wire transfers into the account. Four of the deposits, in the amounts of $2,982.00, $982.00, $5,943.54, and $5,032.00, were from a company called, "ebuygold Ltd."

65. I know, based on my training and experience, that "ebuygold Ltd." is a company based in Hong Kong, China. They offer a currency exchange service. Their service is unique from more mainstream payment services in that they don't convert from U.S. dollars to Euros or other legitimate currencies backed by nation states, but instead exchange from U.S. dollars and other currencies into the electronic currency, "Liberty Reserve."

66. I know from my training and experience that Liberty Reserve is an unregulated web currency based in Costa Rica. I also know from my training and experience that if a person has a Liberty Reserve account, they are able to transfer funds from their account to the account of another Liberty Reserve account holder. The U.S.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Government is unable to obtain records related to these transfers. I know, as well, that Liberty Reserve is one of the primary methods used by the online criminal underworld to transfer money, because of the anonymity that it offers. I also know from my training and experience that legitimate international financial transfers do not use Liberty Reserve because there is no real method of recourse. If money disappeared from the system, there is no verified backing to the system or regulating entity.

67. In April of 2011, there were $58,053.00 in deposits into the Christopher Schroebel account and $26,225.68 in withdrawals. The deposit activity included 13 counter credit deposits, ranging from $200 to $1800 dollars, and eight wire transfers from ebuygold, in the following amounts: $7,804.00, $982.00, $3,782, $7,857.00, $4,982.00, $2,180.00, $982.00 and $1082.00.

68. In May of 2011, there were $10,215.44 in deposits into the account. All of the deposits were transfers from the saving account.

69. In June of 2011, there were $17,684.54 in deposits into the account. There were 11 counter credits in amounts ranging from $200.00 to $1,500.00. There were three transfers from savings and there were two wire transfers from ebuygold, in the amounts of $2,082.00 and $1282.00.

70. In July of 2011 there were three deposits into the account. One was a wire transfer from ebuygold in the amount of $1042.00, and the other two were transfers from savings.

71. In August of 2011 there were four deposits into the account, totaling $1069.00. All four were counter deposits.

72. Based on my review of the bank records, in light of my training and experience, I believe that the records indicate two things:

73. First, regarding the counter deposits - it is notable that the amounts of these deposits match up with the type of "even dollar" cash amounts commonly withdrawn from compromised bank accounts. I believe that Christopher Schroebel is most likely accessing and withdrawing funds from compromised accounts by using the credit card

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

account numbers stolen from hacks like that made to the systems of businesses like Mondello's restaurant and The Seattle Restaurant Store, which he has reencoded onto other plastic cards which he then uses to withdraw cash from the compromised accounts. I know, from my training and experience, that this is one of the fastest ways to turn stolen credit card information into cash.

74. Second, I believe that the wire transfers into Schroebel's account from ebuygold most likely reflect the sale, by him, of the stolen bank information that is being collected on the server with IP address 74.208.193.165. I believe that Christopher Schroebel is selling that information, in bulk, in criminal credit card forums, and receiving his payments via Liberty Reserve, which he is then exchanging at ebuygold, for transfer to his Bank of America Account. This is consistent with my own experience, and that of other law enforcement agents working in this area - that is, when we have visited "carding" forums and then purchased stolen financial information in an undercover capacity in furtherance of criminal investigations, we are usually given the option to use three methods of payment, Liberty Reserve, Web Money and Western Union.

Hack of Computer System in Mamaroneck, NY

75. On October 18, 2011, I reviewed data from a trap and trace device installed on the server located at IP 74.208.193.165. That data showed approximately 50 computers that were connecting to the server using the FTP protocol. Since I knew from my investigation this is the protocol used to transfer stolen credit card data to the server, I theorized that computers connecting to the server and using that protocol are victims of hacks and data theft. I determined that one of the computers connecting to the server and using the FTP protocol belonged to a business named Miller Toys, in Mamaroneck, NY. I contacted the Mamaroneck Police Department, and a subsequent investigation by the Mamaroneck Police Department, American Express, and myself has confirmed a point of sale network intrusion on this business. Records on the other IP addresses have been requested, but in the interim, based on my experience, I believe that all of these IP addresses represent infected point of sale systems.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Control and Use of Computer Server

76. Based on the records obtained from 1&1 Internet, there appear to be two users of the computer server located at IP address 74.208.193.165. Those users being Christopher Schroebel and Peter Schroebel. Based on investigative work that I, and other investigators have done, we believe that Peter Schroebel is Christopher Schroebel's father. Records related to e-mail communications between 1&1 Internet and Peter Schroebel indicate that he does exert some control over this server and is able to access it, and also that he is aware of multiple and repeated complaints regarding abuses that have been connected to the server. The investigation has revealed numerous other facts, however, that indicate it is Christopher Schroebel who is actively engaging in illegal activities using this server and that he paid for this server himself.

77. While there appears to be a small amount of activity on this website that is not related directly to intrusions and the transfer of stolen credit card data, it does appear that all of the activity is directly related, in one way or another, to the Schroebel family. For example, I have determined from my investigation that there is at least one other website hosted on this server, aside from www.scripters.in, and www.crypter.in. The other website is named "Globalherbal.com," and is a website that advertises the sale of "herbal remedies." I know from my investigation in this case that the Schroebel family has used the Internet to heavily advertise and to sell herbal treatments, primarily for "penis enlargement."

78. As part of the investigation, I have done an analysis of the traffic to the server that is located at IP address 74.208.193.165. Based on the data I have accessed for that analysis, I have determined that, in total, over 86% of the traffic to the server involves FTP communications, which is the type of communication used to transfer stolen credit card data, as described above. The other significant component of the traffic (about 10%) consists of "name resolution," which is in essence an Internet "traffic direction" function which has nothing to do with delivering content. I have determined that less

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

than one half of one percent of the traffic to the server is traffic to any website on the server that could possibly involve the delivery of website content.

Search of Computer Server at IP Address 74.208.193.165

79. On October 28, 2011, three search warrants were authorized as part of this investigation. Two of those warrants were authorized by Magistrate Judge James P. Donohue, in the Western District of Washington, the first for the e-mail account UPG.USA@gmail.com, and the second for the computer server located at IP address 74.208.193.165. A third warrant was issued by a Magistrate Judge in the District of Maryland, to search the residence of Christopher Schroebel in Keedysville, MD.

80. Pursuant to the search warrant for the server at IP address 74.208.193.165, I received a copy of the forensic image from that server. I subsequently searched the server and discovered the following:

a) I recovered over 4800 unique credit card tracks from Visa, Mastercard, DiscoverCard and American Express credit cards. The card data was stored as reports from the Ardamax keystroke logger software and matched the manner in which the cards had been stolen from Mondello's restaurant, the Seattle Restaurant store, and others.

b) I recovered 29 executable malware programs. These files were located on the server in a location that would deliver them for download if a person were to type in the web address, www.scripters.in followed by the name of the malware. This is the manner in which the malware was downloaded to the server at Mondello's restaurant. Of the 29 pieces of malware, an initial scan of the files flagged 27 of them as malware.

c) I recovered numerous notes and programs that could be used to scan for remote access, to break into protected computer systems, and to alter computer systems once a person has access to a computer. Specifically, I located commands that could be copied on to a victim computer. Those commands could then be used to turn Remote Desktop either on or off. I also located programs with names like, "rdp_bruters", a program name that indicates it is intended for brute force attacks to gain access to

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Remote Desktop Connections. I found a zipped file titled, "poshackxxx.bak.zip," which I read to say, "POS HACK XXX BACKUP." I extracted the files from inside this zip archive and located all of the tools necessary to gain access to a protected Point of Sale (POS) system, as well as programs for breaking the password protected systems. I located dictionary files on known passwords that could be used with those files.

d) Finally, I located a program that I have seen in another investigation that is used to to scan large ranges of IP addresses in search of computers that may be vulnerable to a Remote Desktop attack.

Search and Interview of Peter Schroebel

81. The search warrant for the residence of Christopher Schroebel was executed on October 28, 2011 by agents of the USSS. The executing agents met and spoke with Peter Schroebel at the time of the search. Peter Schroebel told the agents that his son, Christopher, had moved out of their house in recent months, but that a number of his computers remained in the house.

82. The executing agents seized several dozen computer systems from the residence. That evidence has now been shipped to the USSS Seattle Field Office for forensic examination.

83. On November 14, 2011, I interviewed Peter Schroebel by telephone. He provided information to me that included the following:

a) Christopher Schroebel is heavily involved in intravenous heroin use and is currently staying with a girlfriend in Maryland.

b) Christopher Schroebel had been in phone contact with Peter Schroebel after the 1&1 Internet web hosting server had been searched and taken offline. Christopher wanted his father to help him get the server back online.

c) Christopher Schroebel was now using a server in Luxemborg.

84. As part of my investigation, I had independently discovered that, in the weeks since the 1&1 Internet server was taken down on October 29, 2011, Christopher Schroebel had reestablished his servers for www.scripters.in and www.crypter.in on a

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

webserver with an IP address that traced to a hosting provider located in Luxemborg. Relocating the websites to a Luxemborg hosting company has made it more difficult for U.S. law enforcement to intervene with criminal activity conducted from that server location.

E. Conclusion

Based on the above facts, I respectfully submit that there is probable cause to believe that CHRISTOPHER SCHROEBEL has committed violations of Title 18, United States Code, Sections 1030(a)(2), 1030(c)(2)(B)(ii); 1029(a)(2); 1029(c)(1)(A)(i) and 1028A(a)(1).

David Dunn, Complainant
Seattle Police Department Detective
Officer, USSS E-Crimes Task Force

Based on the Complaint and Affidavit sworn to before me, and subscribed in my presence, the Court hereby finds that there is probable cause to believe the Defendant committed the offenses set forth in the Complaint.

Dated this 16th day of November 2011.

BRIAN A. TSUCHIDA
United States Magistrate Judge

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970